Fehlerbehebung bei Multicast-Datenverkehr, der nicht über die FTD-Firewall läuft, mit Bidir PIM-Konfiguration

Inhalt

Problem

Alle diese Symptome treten auf:

- Der Multicast-Datenverkehr funktioniert auf der Firewall Threat Defense (FTD) für eine bestimmte Multicast-Gruppe nicht mehr.
- In der FTD für die Gruppe sind keine Multicast-Routen (in diesem Beispiel 224.2.2.2) vorhanden.

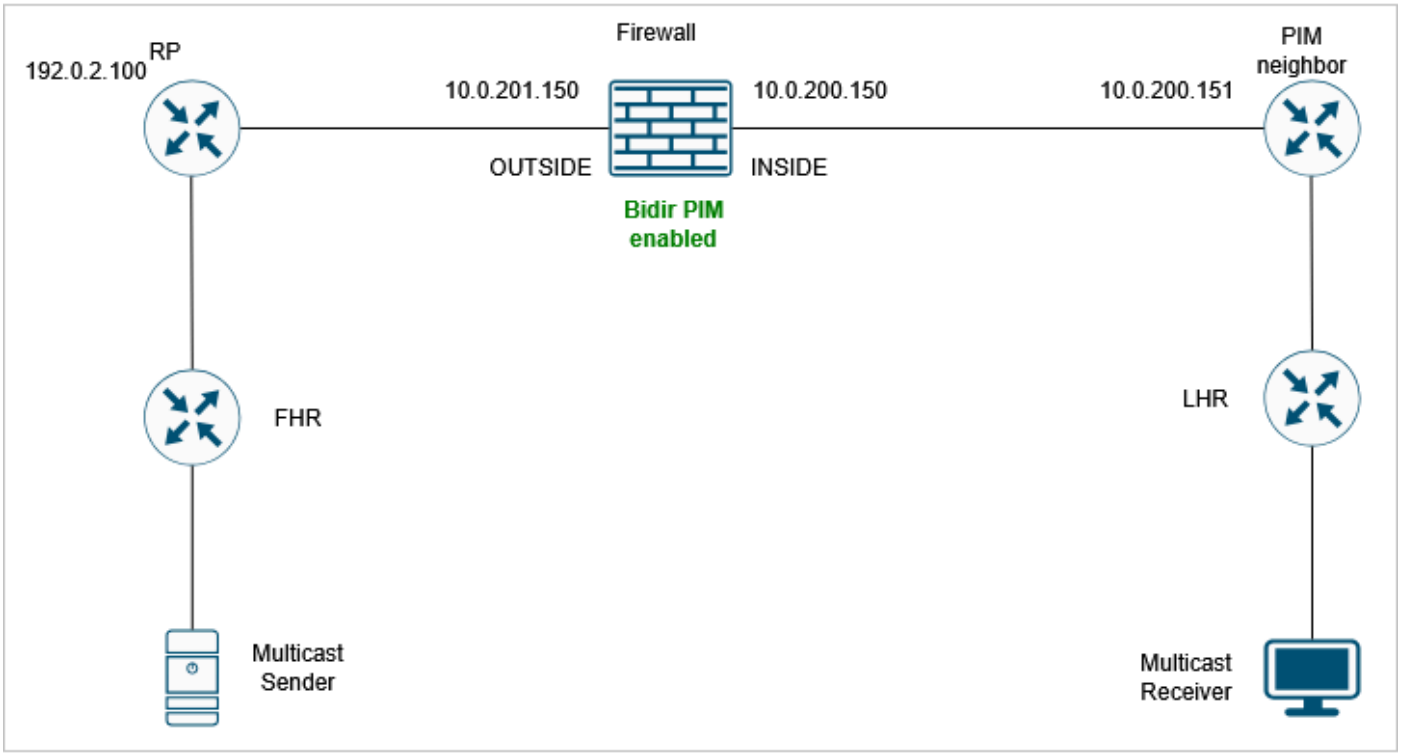
<#root>

```
device#

show mroute 224.2.2.2


No mroute entries found.
device#
```

Umwelt

- Zuerst gesehen in FTD Version 7.4. Andere Softwareversionen, einschließlich Adaptive Security Appliance (ASA), können ebenfalls betroffen sein.
- Bidirectional Protocol Independent Multicast (PIM) ist auf der Firewall aktiviert.

Topologie



inline_image_0,png

Auflösung

Schritt 1: Überprüfen der aktuellen Multicast-Konfiguration

Untersuchen der vorhandenen Multicast-Routing-Konfiguration auf allen Geräten im Netzwerkpfad, um mögliche Fehlkonfigurationen oder fehlende Einstellungen zu ermitteln, die verhindern könnten, dass Multicast-Datenverkehr die Firewall passiert.

Die Firewall verfügt über eine bidirektionale PIM-Konfiguration:

<#root>

```
device#
```

show run pim

```
pim rp-address 192.0.2.100 bidir
```

Phase 2: Überprüfen der PIM-Nachbarn

Vergewissern Sie sich, dass die Multicast-Nachbarn ordnungsgemäß auf der Firewall angezeigt werden:

<#root>

```
device#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
10.0.200.151      INSIDE             19:13:30  00:01:24 1 (DR)
10.0.201.200      OUTSIDE            00:01:31  00:01:42 1 (DR)

B
```

In der Ausgabemeldung hat Nachbar 10.0.201.200 das BiDir B-Flag, während Nachbar 10.0.200.151 es nicht hat.

Schritt 3: PIM-Debugging für Multicast-Gruppe 224.2.2.2 aktivieren:

<#root>

```
FPR3100-14#

debug pim group 224.2.2.2


IPv4 PIM group debugging is on
 for group 224.2.2.2
```

Das Debugging zeigt, dass ein PIM-Join/Prune-Paket vorhanden ist, das aufgrund von "no bidir df election" verworfen wird:

<#root>

```
IPv4 PIM: J/P entry: Join root: 192.0.2.100 group: 224.2.2.2 flags:  RPT WC S
IPv4 PIM: (*,224.2.2.2) J/P with RP 192.0.2.100 on INSIDE
```

discarded, no bidir df election-state on this intf

Schritt 4: Aktivieren Sie PIM-Erfassungen für den PIM-Nachbarn 10.0.200.151. Das Ziel besteht darin, mehr Transparenz für den Paketinhalt zu erhalten:

<#root>

```
device#
```

capture CAPI interface INSIDE trace match pim host 10.0.200.151 any

Schritt 5: Erfassen Sie die Firewall-Erfassung vom FTD-Gerät:

<#root>

```
device#
```

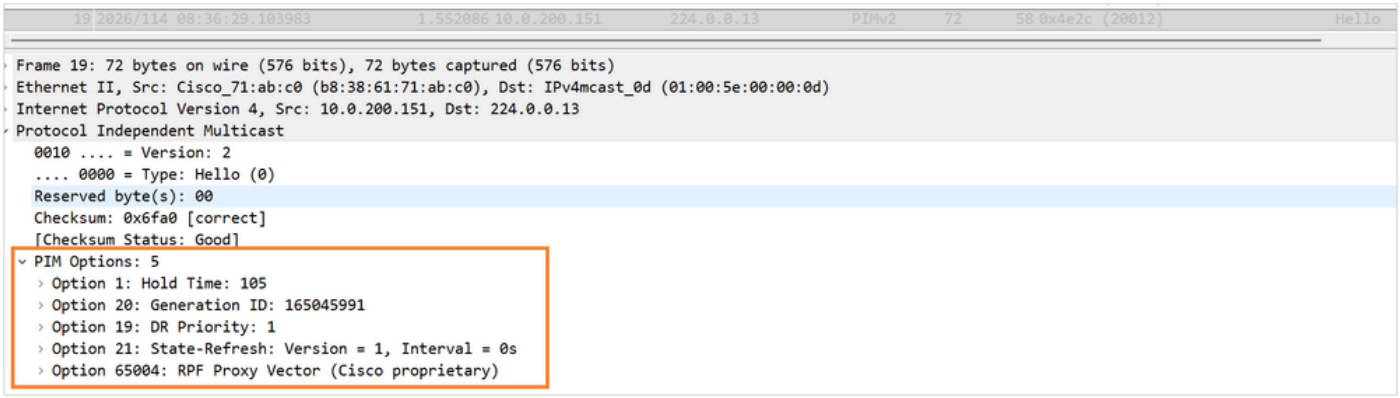
copy /pcap capture:CAPI CAPI.pcap

```
Source capture name [CAPI]?
Destination filename [CAPI.pcap]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
!
28 packets copied in 0.0 secs
```

Sammeln Sie die pcap-Datei vom FMC, indem Sie das unter https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html beschriebene Verfahren verwenden.

Schritt 6: Erfassungsanalyse.

Das PIM Hello-Paket enthält folgende Optionen:



PIM_Hello_Options_no-bidir-fähig.png

Beachten Sie, dass das BiDir-fähige Flag nicht vorhanden ist.

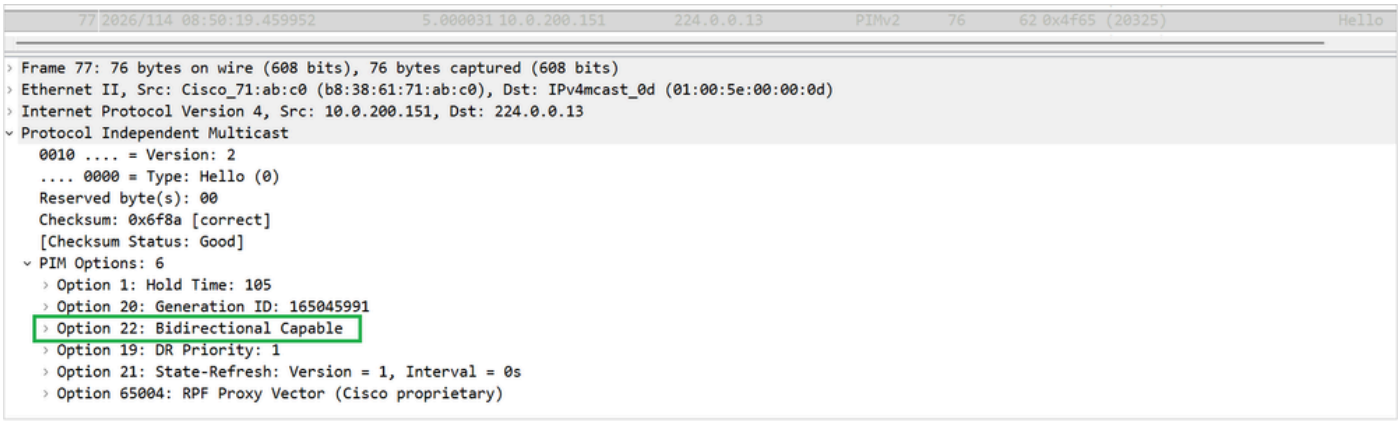
Schritt 7: Aktivieren Sie das bidirektionale PIM auf dem 10.0.200.151-Nachbarn.

Jetzt wird für beide Nachbarn das PIM BiDir B-Flag angezeigt:

<#root>

```
device#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
10.0.200.151      INSIDE             19:34:26  00:01:38 1 (DR)

B


10.0.201.200      OUTSIDE            00:22:27  00:01:23 1 (DR) B
```

Schritt 8: Erfassen Sie eine neue Erfassung, und überprüfen Sie die PIM Hello-Optionen für Nachbar 10.0.200.151. Die PIM-Option 22 (Bidirectional Capable) wird angezeigt:



PIM_Hello_Options_option22.png

Schritt 9: Stellen Sie sicher, dass jetzt die Mroute für die Multicast-Gruppe 224.2.2.2 angezeigt wird:

<#root>

device#

show mroute

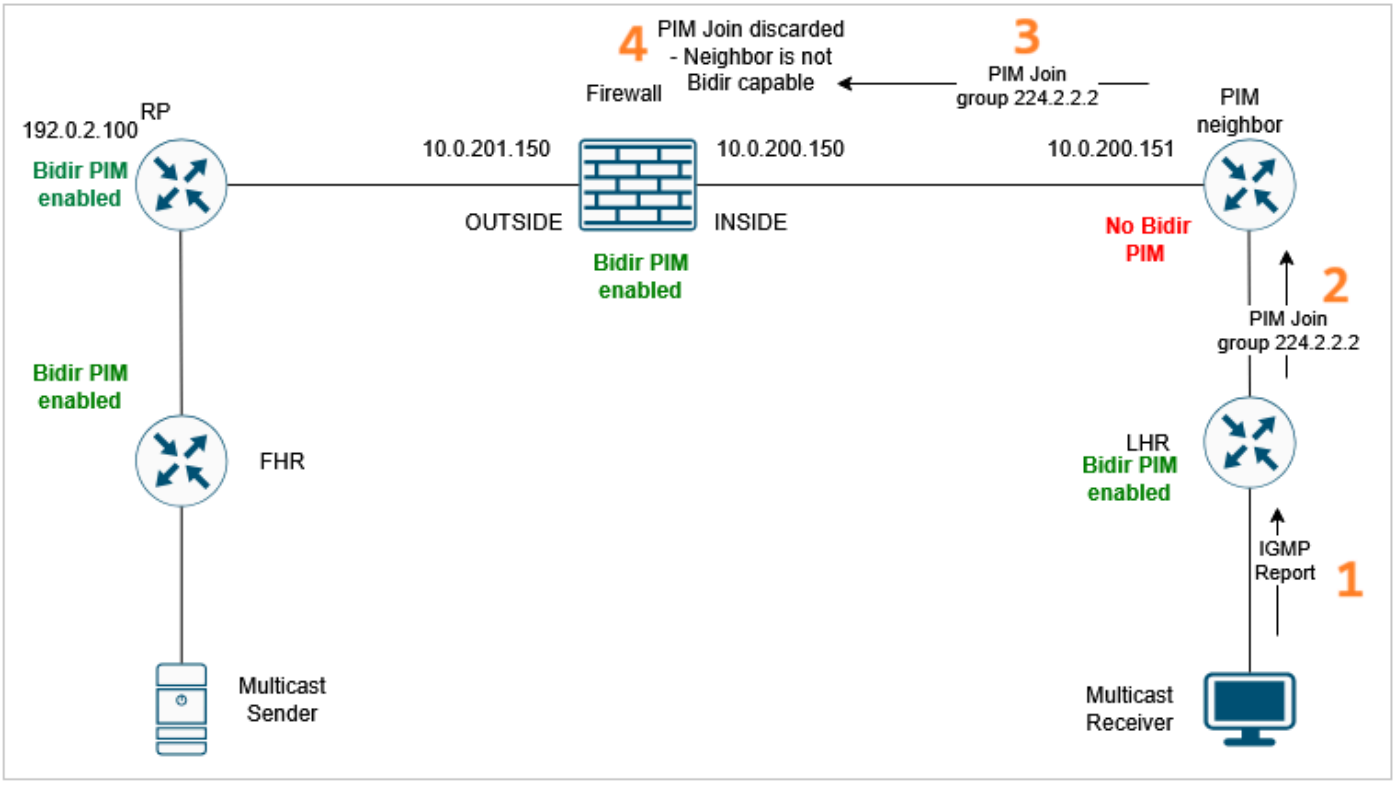
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
(*, 224.0.1.40), 19:41:44/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:
    INSIDE, Null, 19:41:44/never
```

(*, 224.2.2.2)

```
, 00:06:29/00:02:53, RP 192.0.2.100, flags: B
  Bidir-Upstream: OUTSIDE
  RPF nbr: 10.0.201.200
  Immediate Outgoing interface list:
    INSIDE, Forward, 00:06:29/00:02:53
```

Ursache

Der Ausfall des Multicast-Datenverkehrs wurde durch eine falsche oder unvollständige Multicast- und bidirektionale PIM-Konfiguration auf dem benachbarten Netzwerkgerät verursacht. Das spezifische Konfigurationsproblem führte dazu, dass die PIM-Join/Prune-Nachricht für die spezifische Multicast-Gruppe von FTD verworfen wurde. Daher konnte die Firewall die Route für den Multicast-Verkehr nicht erstellen. Damit Multicast-Datenverkehr durch die Firewall-Datenebene fließen kann, muss die Kontrollebene (PIM) die korrekte Mroute festlegen.



Ursache.png

Verwandte Inhalte

- https://datatracker.ietf.org/doc/html/rfc5015#section-3.7.4

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.